

UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Apple Records Associated with Apple ID
doudzme@icloud.com

Case No. 1:17sw

475

JUL 28 2017

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. §§ 371, 793, 794,
951 and 1956

Offense Description
Conspiracy, Gathering, transmitting or losing defense information,
Gathering or delivering defense information to aid a foreign government, Agent of a
Foreign Government, Laundering of monetary instruments

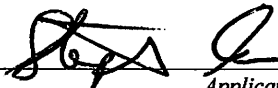
The application is based on these facts:

See Attached Affidavit

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA/SAUSA:

AUSA John T. Gibbs



Applicant's signature

Stephen Green, FBI Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 07/28/2017

/s/ Theresa Carroll Buchanan
United States Magistrate Judge

Judge's signature

City and state: Alexandria, Virginia

Theresa C. Buchanan, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Apple ID doudzme@icloud.com (the “account”) that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber

Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

- f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging and query logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);
- g. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;
- h. All records pertaining to the types of service used;
- i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and
- j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

II. Information to be seized by the government

All information described above in Section I that constitutes contraband, fruits, evidence and/or instrumentalities of violations of 18 U.S.C. § 371, 18 U.S.C. § 793, 18 U.S.C. § 794, 18 U.S.C. § 1956, and 18 U.S.C. § 951, involving Kevin Patrick Mallory **from October 13, 2011 to the present**, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Communications between Kevin Patrick Mallory and anyone associated with a foreign government;
- b. Any communications, files or other records containing information relating to the national defense and/or classified information;
- c. Any communications, files or other records containing U.S. Government information;
- d. Any communications, files or other records regarding tradecraft, how to obtain or deliver sensitive information, and/or how to avoid or evade detection by intelligence officials or law enforcement authorities;
- e. Any communications, files or other records regarding travel, including calendars, travel tickets, receipts, and photographs;
- f. Any communications, files or other records pertaining to any others who conspired with Kevin Patrick Mallory to release, communicate, or transmit national defense information and/or classified information;

g. Any financial records, including bank statements, account information and records of any financial transaction that may be evidence of payments for the sale of classified information;

h. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

i. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

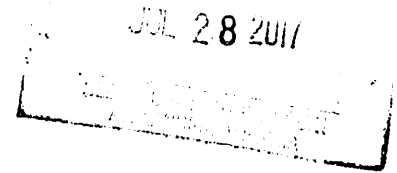
j. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

k. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

l. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN THE MATTER OF THE SEARCH OF)
INFORMATION ASSOCIATED WITH)
APPLE ID DOUDZME@ICLOUD.COM)
THAT IS STORED AT PREMISES)
CONTROLLED BY APPLE, INC.)

CASE NO. 1:17 sw 475

UNDER SEAL

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Stephen Green, after being duly sworn, depose and state as follows:

1. I am a Special Agent with the FBI, and have been since 2012. Since 2012, I have been assigned to the Washington Field Office, Counterintelligence Division. Since October 2016, I investigated offenses involving espionage and the unlawful retention or disclosure of classified information. I was the affiant on the affidavit in support of a criminal complaint and arrest warrant, charging Kevin Patrick Mallory (hereinafter Mallory) with making materially false statements to Federal Bureau of Investigation (FBI) agents, in violation of 18 U.S.C. § 1001, and Gathering or Delivering Defense Information to Aid a Foreign Government, in violation of 18 U.S.C. § 794.

2. This affidavit is submitted in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with the above-listed Apple ID that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop,

Cupertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

3. Based on the facts set forth in this affidavit (and incorporating the facts contained in the Criminal Complaint Affidavit), there is probable cause that within these locations or things is evidence, more particularly described in Attachment A, of violations of federal law, including 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 793(e) (gathering, transmitting or losing defense information), 18 U.S.C. § 794(a) (gathering or delivering defense information to aid foreign government), 18 U.S.C. § 1956 (laundering of monetary instruments) and 18 U.S.C. § 951 (agent of a foreign government).

4. This affidavit is being submitted for the limited purpose of obtaining a search warrant. As a result, it does not include each and every fact observed by me or known to the government. When I assert that a statement was made by an individual, that statement is described in substance and in part, but my assertion is not intended to constitute a verbatim recitation of the entire statement. When I assert that an event occurred or a communication was made on a certain date, I mean that the event occurred or the communication was made “on or about” that date.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

INFORMATION REGARDING APPLE ID AND iCloud¹

6. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

7. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

¹ The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; “Create and start using an Apple ID,” available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “iCloud: iCloud storage and backup overview,” available at <https://support.apple.com/kb/PH12519>; and “iOS Security,” available at http://images.apple.com/privacy/docs/iOS_Security_Guide.pdf.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be

purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

8. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and synching mechanism.

9. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or AOL). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

10. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to

and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

11. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s website. Apple also maintains records reflecting a user’s app purchases from App Store and iTunes Store, “call invitation logs” for FaceTime calls, and “mail logs” for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

12. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user’s IP address and identifiers such as the Integrated Circuit Card ID number (“ICCID”), which is the serial number of the device’s SIM card. Similarly, the telephone number of a user’s iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address (“MAC address”), the unique device identifier (“UDID”), and the serial number. In addition, information about a user’s computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user’s web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including

communications regarding a particular Apple device or service, and the repair history for a device.

13. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

PROBABLE CAUSE

14. On or about June 19, 2017, in response to a subpoena request, Apple provided information that the Apple account doudzme@icloud.com is associated with Apple DS ID 12822856 and is registered to Mallory at his residence of 16621 Elk Run Ct, Leesburg, Virginia. The account was created on October 13, 2011 and is currently active. Also, at the time of his

arrest on June 22, 2017, Mallory's personal iPhone 5 was seized. A search of that phone showed the account doudzme@icloud.com listed under the contact "Kevin Mallory."

15. During Mallory's secondary search and interview on April 21, 2017 with Customs and Border Protection agents following a flight from Shanghai, China, Mallory was found to be traveling with two Apple iPhones. Mallory later admitted to the FBI in an interview on May 24, 2017, that he had met with a person he believed was a People's Republic of China government agent ("PRC1") while on that April trip to China. Given the presence of two Apple iPhones in his possession after this trip to China in May, and given his admission that he had met with someone he believed to be a Chinese government agent, there is probable cause to believe that information related to this trip will be found in a search of the Apple account doudzme@icloud.com.

16. In my training and experience, evidence of who was using an Apple ID, where they were located when they were using an Apple ID, and evidence related to the criminal activity of the kind described above, may be found in the Apple files and records for the doudzme@icloud.com account.

17. I know that Mallory has transmitted classified documents to PRC1. Given that Mallory previously worked at the U.S. government agency that classified these documents, and given that these documents are several years old, I believe that it is likely that Mallory maintains other documents related to his employment with the U.S. Government connected to his Apple ID. The stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation, to include 18 U.S.C. §§ 371, 793(e), 794(a), 1956 and 951. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and

documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

18. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

19. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

20. During the May 24 meeting with the FBI agents, Mallory signed a voluntary consent form permitting the FBI to search the device provided to Mallory by PRC1, which he had brought to the meeting. At that time, the FBI extracted an image of the device, and returned the device to Mallory. The FBI conducted further technical examination of the imaged copy of

the device after the interview. Identified on the device was a series of messages sent on or about May 3, 2017, where Mallory stated, "I have arranged for a USD account in another name. You can send the funds broken into 4 equal payments over 4 consecutive days...When you agree I will send you the bank I.g instructions." Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services, such as banking institutions, used in furtherance of the crimes under investigation or services used to communicate with PRC1. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

21. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

22. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION


23. Based on the forgoing, I request that the Court issue the proposed search warrant.

24. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING


25. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,



Stephen Green
Special Agent
Federal Bureau of Investigation
Washington, DC

Subscribed and sworn to before me on July 28, 2017



/s/ Theresa Carroll Buchanan
United States Magistrate Judge

THE HONORABLE THERESA C. BUCHANAN
UNITED STATES MAGISTRATE JUDGE

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
BUSINESS RECORDS PURSUANT TO FEDERAL RULE
OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Apple Inc., and my official title is _____. I am a custodian of records for Apple Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Apple Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Apple Inc.; and
- c. such records were made by Apple Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Apple ID doudzme@icloud.com (the “account”) that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber

Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging and query logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

g. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

II. Information to be seized by the government

All information described above in Section I that constitutes contraband, fruits, evidence and/or instrumentalities of violations of 18 U.S.C. § 371, 18 U.S.C. § 793, 18 U.S.C. § 794, 18 U.S.C. § 1956, and 18 U.S.C. § 951, involving Kevin Patrick Mallory **from October 13, 2011 to the present**, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Communications between Kevin Patrick Mallory and anyone associated with a foreign government;
- b. Any communications, files or other records containing information relating to the national defense and/or classified information;
- c. Any communications, files or other records containing U.S. Government information;
- d. Any communications, files or other records regarding tradecraft, how to obtain or deliver sensitive information, and/or how to avoid or evade detection by intelligence officials or law enforcement authorities;
- e. Any communications, files or other records regarding travel, including calendars, travel tickets, receipts, and photographs;
- f. Any communications, files or other records pertaining to any others who conspired with Kevin Patrick Mallory to release, communicate, or transmit national defense information and/or classified information;

g. Any financial records, including bank statements, account information and records of any financial transaction that may be evidence of payments for the sale of classified information;

h. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

i. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

j. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

k. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

l. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia

JUN 21 2017

United States of America
v.
KEVIN PATRICK MALLORY

Case No. 1:17-MJ-288

Defendant(s)

FILED UNDERSEAL

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of April 1, 2017 through May 31, 2017 in the county of Loudoun in the
Eastern District of Virginia, the defendant(s) violated:

Code Section

Offense Description

18 U.S.C. § 1001
18 U.S.C. § 794

Making materially false statements to the FBI
Gathering or delivering defense information to aid a foreign government

This criminal complaint is based on these facts:

SEE ATTACHED AFFIDAVIT

☒ Continued on the attached sheet.

Reviewed by AUSA/SAUSA:

AUSA JOHN GIBBS



Complainant's signature

Stephen Green, Special Agent FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: June 21, 2017

City and state: Alexandria, VA

/s/

Theresa Carroll Buchanan

United States Magistrate Judge

Judge's signature

Theresa C. Buchanan, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

JUN 21 2017

UNITED STATES OF AMERICA,

v.

KEVIN PATRICK MALLORY,

Defendant

)
)
)
)
)
)
)

Case No: 1:17mj 288

UNDER SEAL

GOVERNMENT'S MOTION TO SEAL CRIMINAL COMPLAINT
AND ARREST WARRANT PURSUANT TO LOCAL RULE 49(B)

The United States, by and through undersigned counsel, pursuant to Local Rule 49(B) of the Local Criminal Rules for the United States District Court for the Eastern District of Virginia, asks for an Order to Seal the criminal complaint and arrest warrant until the defendant is arrested.

I. Reasons for Sealing (Local Rule 49(B)(1))

1. The United States seeks to arrest the defendant on a criminal complaint. The investigators suspect that, if the defendant were to learn of the criminal complaint, he would destroy evidence and/or flee. Sealing the criminal complaint and arrest warrant may enable the investigators to arrest the defendant by preventing the disclosure of the complaint and warrant from causing the defendant to destroy evidence and/or flee.

2. Premature disclosure of the charge against the defendant would jeopardize an ongoing criminal investigation by threatening our ability to seize evidence and arrest the defendant. Disclosure of the complaint and arrest warrant would apprise the defendant of the pending charges and encourage his flight to avoid prosecution. Wherefore, we seek to seal the

complaint and arrest warrant pending defendant's arrest.

II. References to Governing Case Law (Local Rule 49(B)(2))

3. Sealing an indictment is appropriate to allow the government to complete an investigation properly. *United States v. Ramey*, 791 F.2d 317, 320-21 (4th Cir. 1986). *See, e.g., United States v. Wright*, 343 F.3d 849, 858 (6th Cir. 2003); *United States v. DiSalvo*, 34 F.3d 1204 (3rd Cir. 1994). The Court has the inherent power to seal affidavits in support of warrants to protect an ongoing investigation. *See United States v. Wuagneux*, 683 F.2d 1343, 1351 (11th Cir. 1982); *Times Mirror Company v. United States*, 873 F.2d 1210 (9th Cir. 1989).

4. "The trial court has supervisory power over its own records and may, in its discretion, seal documents if the public's right of access is outweighed by competing interests." *In re Knight Pub. Co.*, 743 F.2d 231, 235 (4th Cir. 1984). Sealing affidavits is appropriate where there is a substantial probability that release of the sealed documents would compromise the government's on-going investigation. *See e.g. In re Search Warrant for Secretarial Area Outside Office of Gunn*, 855 F.2d 569, 574 (8th Cir. 1988); *Matter of Eye Care Physicians of America*, 100 F.3d 514, 518 (7th Cir. 1996).

5. Sealing should be narrowly tailored to balance the values furthered by sealing (including the protection of ongoing criminal investigations) against the values furthered by unsealing (including the enhancement of the public's ability to evaluate the performance of the investigators). *Baltimore Sun v. Goetz*, 886 F.2d 60, 65-66 (4th Cir. 1989). In this case, the investigation cannot be protected without sealing the criminal complaint and arrest warrant.

III. Period of Time Government Seeks to Have the
Matter Remain Under Seal (Local Rule 49(B)(3))

6. The criminal complaint and arrest warrant may need to remain sealed until the defendant is arrested. Pursuant to Local Rule 49(B)(3), the sealed materials should automatically be unsealed and handled after the defendant is arrested.

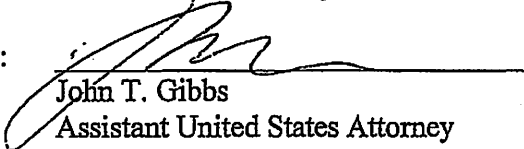
7. The United States has considered alternatives less drastic than sealing and has found none that would suffice to protect this investigation.

WHEREFORE, the United States respectfully requests that the criminal complaint and arrest warrant and this Motion to Seal and proposed Order be sealed until the defendant is arrested.

Respectfully submitted,

Dana J. Boente
United States Attorney

By:


John T. Gibbs
Assistant United States Attorney

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

JUN 21 2017

UNITED STATES,

v.

KEVIN PATRICK MALLORY

Defendant

Case No.: 1:17mj-280

UNDER SEAL

ORDER TO SEAL

The UNITED STATES, pursuant to Local Rule 49(B) of the Local Criminal Rules for the United States District Court for the Eastern District of Virginia, having moved to seal the criminal complaint, the arrest warrant, the Motion to Seal, and proposed Order in this matter; and

The COURT, having found that revealing the material sought to be sealed would jeopardize an ongoing criminal investigation; having considered the available alternatives that are less drastic than sealing, and finding none would suffice to protect the government's legitimate interest in concluding the investigation; and finding that this legitimate government interest outweighs at this time any interest in the disclosure of the material; it is hereby

ORDERED, ADJUDGED, and DECREED that the criminal complaint, arrest warrant, Motion to Seal, and this Order be Sealed until the defendant is arrested, at which point all those documents will be unsealed without further order of the Court. /s/

Theresa Carroll Buchanan
United States Magistrate Judge
THERESA CARROLL BUCHANAN
UNITED STATES MAGISTRATE JUDGE

Date: 6/21/17
Alexandria, Virginia

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

JUN 21 2017

UNITED STATES OF AMERICA

v.

KEVIN PATRICK MALLORY,

Defendant

) UNDER SEAL

) Criminal No. 1:17-cr-288

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A CRIMINAL COMPLAINT AND ARREST WARRANT

I, Stephen Green, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the FBI, and have been since 2012. Since 2012, I have been assigned to the Washington Field Office, Counterintelligence Division. Since October 2016, I have investigated offenses involving espionage and the unlawful retention or disclosure of classified information.

2. I have training in the preparation, presentation, and service of criminal complaints, and have been involved in the investigation of numerous types of offenses against the United States. I have also been trained in the preparation, presentation, and service of arrest and search warrants, and have executed both arrest warrants and search warrants in previous cases.

3. The facts in this affidavit are based on my personal observations, my training and experience, and information obtained from other witnesses and law enforcement agents. This affidavit is intended to show merely that there is sufficient probable cause for the requested criminal complaint and warrant and does not set forth all of my knowledge about this matter.

PURPOSE OF AFFIDAVIT

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that Mallory violated 18 U.S.C. § 1001 (Making Material False Statements) and 18 U.S.C. § 794 (Gathering or Delivering Defense Information to Aid a Foreign Government). I therefore make this affidavit in support of a criminal complaint charging Mallory with these offenses.

STATUTORY AUTHORITY AND DEFINITIONS

5. For the reasons set forth below, there is probable cause to believe that Mallory committed violations of Title 18, United States Code, Section 1001, and Title 18, United States Code, Section 794(a).

6. Under 18 U.S.C. § 1001, “whoever, in any matter within the jurisdiction of the executive, legislative or judicial branch of the Government of the United States, knowingly and willfully makes any materially false, fictitious, or fraudulent statement or representation” shall be fined or imprisoned for a term of not more than five years.

7. Under 18 U.S.C. § 794(a), “whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers or transmits, or attempts to communicate, deliver or transmit, to any foreign government . . . or to any representative, officer, agent, employee, subject, or citizen thereof . . . any document, writing, . . . or information relating to the national defense” shall be imprisoned “for any term of years or for life[.]”

8. Under Executive Order 13526, information in any form may be classified if it: (1) is owned by, produced by or for, or is under the control of the United States Government; (2) falls within one or more of the categories set forth in the Executive Order [Top Secret, Secret, and

Confidential]; and (3) is classified by an original classification authority who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security.

9. Where such unauthorized disclosure could reasonably result in damage to the national security, the information may be classified as "Confidential" and must be properly safeguarded. Where such unauthorized disclosure could reasonably result in serious damage to the national security, the information may be classified as "Secret" and must be properly safeguarded. Where such unauthorized disclosure could reasonably result in exceptionally grave damage to the national security, the information may be classified as "Top Secret" and must be properly safeguarded.

10. Classified information of any designation may be shared only with persons determined by an appropriate United States Government official to be eligible for access, and who possess a "need to know." Among other requirements, in order for a person to obtain a security clearance allowing that person access to classified United States Government information, that person is required to and must agree to properly protect classified information by not disclosing such information to persons not entitled to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations. If a person is not eligible to receive classified information, classified information may not be disclosed to that person. In order for a foreign government to receive access to classified information, the originating United States agency must determine that such release is appropriate.

PROBABLE CAUSE

Relevant Parties:

11. Kevin Patrick Mallory is a 60-year-old self-employed consultant with GlobalEx, LLC. He is a United States citizen who resides and works at 16621 Elk Run Court, Leesburg, Virginia 20176. Mallory graduated from Brigham Young University in 1981 with a B.A. degree in Political Science. After graduation, Mallory worked full time in an active duty military position until 1986. After he left active duty, Mallory continued his military service as an Army reservist. From 1987 through 1990, Mallory worked as a Special Agent for the State Department Diplomatic Security Service. From 1990 to 2013, Mallory worked at various government agencies, for U.S. cleared defense contractors, and on U.S. Army active duty deployments. Mallory was stationed in locations including Iraq, the People's Republic of China ("PRC"), Taiwan, and the greater Washington D.C. area. During much of that time, Mallory held a TOP SECRET security clearance. Mallory has language fluency in Mandarin Chinese.

12. In March and April 2017, while visiting Shanghai, China, Mallory met with an individual (hereinafter "PRC1") who represented himself to Mallory as working for a PRC think tank, the Shanghai Academy of Social Sciences ("SASS").

Chinese Institutions, Intelligence Services and Associated Terms:

13. According to its public website, SASS was "founded in 1958 and administered by the Municipal Government of Shanghai," and "receives most of its funds from the municipal government of Shanghai." According to a 2007 report on Chinese think tanks by the Center for Naval Analysis, a federally funded research and development center, SASS is one of the two largest and most established Shanghai think tanks. That report also noted "all provincial- and

municipal-level think tanks are affiliated with the provincial or municipal government they serve. That government is their primary client.”

14. The FBI has described SASS as a leading think tank and distinguished academic institution that specializes in humanities and social sciences to include economics, history, philosophy, journalism, international relations, and sociology. PRC policy-makers utilize SASS publications. Since at least 2014, the FBI has assessed that the Shanghai State Security Bureau (“SSSB”), a sub-component of the Ministry of State Security (“MSS”), has a close relationship with SASS and uses SASS employees as spotters and assessors. FBI has further assessed that SSSB intelligence officers have also used SASS affiliation as cover identities.

15. The PRC intelligence services (“PRCIS”) encompass both the civilian and military components of Chinese intelligence programs. Civilian intelligence collection is handled by the MSS. The MSS can be described as an institution similar to the FBI and the Central Intelligence Agency (“CIA”) combined under one intelligence directorate responsible for counter-intelligence, foreign intelligence, and political security. The MSS consists of a central ministry, provincial state security departments, and municipal state security bureaus, such as the Beijing State Security Bureau (“BSSB”) and the SSSB.

16. Among other things, the MSS and its regional bureaus are focused on identifying and influencing the foreign policy of other countries, including the United States. The MSS and its bureaus seek to obtain information on political, economic, and security policies that might affect the PRC, foreign intelligence operations directed at the PRC, and biographical profiles of foreign politicians and intelligence officers.

17. Additionally, the MSS and its bureaus are tasked with conducting clandestine and overt human source operations, of which the United States is a principal target. These operations

use trained intelligence officers, as well as non-professional collectors called “cut-outs” or “co-optees.” A cut-out or co-optee is a person trusted by both the source and the intelligence officer who helps to provide a layer of insulation between an intelligence officer and a source, and thereby increases operational security. Cut-outs or co-optees can operate under a variety of covers, posing as diplomats, journalists, academics, or business people both at home and abroad. These individuals are tasked with spotting, assessing, targeting, collecting, and handling sources or assets with access to classified, open-source, proprietary, or sensitive information that the government of the PRC can utilize for economic, political, or military decision-making or advantage. Sources or assets are people who agree to help a foreign intelligence service by providing information to that service in response to taskings from foreign intelligence officers or agents.

18. PRCIS source operations tend to originate inside the PRC, where the PRCIS prefers to meet with its sources or assets. To facilitate continued meetings inside the PRC, the PRCIS will arrange and/or pay for travel and expenses. The PRCIS is known to pay their sources not only in cash, but also through other means, including business considerations or other types of assistance within the PRC.

Mallory's U.S. Government Security Clearances:

19. As required for his various government positions, Mallory obtained a TOP SECRET security clearance, which was active during various assignments during his career. Mallory's security clearance was terminated in October 2012 when he left government service.

20. Because Mallory held a security clearance and was assigned to various government agencies, both as an employee and as a private contractor, the U.S. Government entrusted Mallory with access to sensitive government materials, including information relating to the national

defense that was closely held by the government ("National Defense Information") and classified documents and materials.

Timeline of Mallory's Contacts with Individuals He Believed To Be PRCIS Agents

21. On or about April 21, 2017, after a return flight to the United States from Shanghai, Mallory was subjected to a U.S. Customs and Border Protection ("CBP") secondary search and interview by CBP at Chicago O'Hare Airport. Mallory was informed that CBP policy and procedure dictated that anyone crossing the border was subject to inspection, including an inspection of all of their belongings and electronic devices.

22. During the CBP interview, Mallory stated that he was outside the United States for one week, and he was returning from Shanghai. Mallory stated that it was a business trip as well as a father/son vacation. Mallory stated that he was currently a consultant for "GlobalEx," which was a company he founded in 2010. While in the PRC on this trip, Mallory said he met with an individual whom he knew through Mallory's church, and stated that he was consulting with this individual on anti-bullying/family safety development. Mallory also stated that he did not receive anything from this individual during his trip.

23. Mallory checked "no" in response to question no. 13 on the CBP Customs Declaration Form 6059b, which asked whether he was carrying over \$10,000 in U.S. or foreign currency. CBP, however, found \$16,500 U.S. Dollars ("USD") in Mallory's two carry-on bags. Mallory was allowed to amend his customs declaration to reflect the correct amount of money he was bringing into the United States.

24. On May 24, 2017, Mallory submitted to a voluntary interview with the FBI in Ashburn, Virginia. Mallory told the FBI agents he had been contacted on a social media site by a Chinese recruiter (hereinafter "PRC2") in or around February 2017. Mallory recounted that, over

the next several days, he had phone interviews with PRC2 and was introduced by PRC2 to a potential client (PRC1, discussed above). Mallory told the agents that he travelled to Shanghai separately in March 2017 and April 2017 to meet with PRC1 and PRC1's boss (hereinafter "PRC3").

25. Mallory told the agents that he had reached out in or around March 2017 to one or more former co-workers (to include two individuals, hereinafter "Employee1" and "Employee2") from a U.S. government agency (hereinafter "USGA1") requesting they help him get in contact with a specific department in USGA1. Mallory told agents that Employee1 and Employee2 did not facilitate any contact with the specific department, or anyone at USGA1, as he had requested. Mallory described to the agents how he again contacted Employee1 in April 2017 requesting help arranging a meeting with USGA1 to discuss people Mallory had recently met with in the PRC. Based on its investigation, the FBI knows this contact to have occurred after Mallory was subjected to a secondary search and interview by CBP.

26. Mallory told the agents that Employee1 facilitated a meeting for him at USGA1, which the FBI knows to have been on May 12, 2017, where he met with an employee of USGA1 (hereinafter "Employee3"). Recounting that meeting to the agents, Mallory said that he had informed Employee3 that he now believed that individuals he had met with in Shanghai (previously identified as PRC1 and PRC3) were affiliated with the PRCIS. Mallory stated that he had told Employee3 about receiving a communication device from PRC1, and that he had been trained in how to use it. According to Mallory, he had agreed with Employee3 to meet again with U.S. government employees to allow the device to be technically examined.

27. Mallory told the FBI Agents that he had come to the May 24, 2017 meeting voluntarily, expecting to meet with Employee3. Upon arrival, he was introduced to the FBI agents.

During the May 24 meeting with the FBI agents, Mallory signed a voluntary consent form permitting the FBI to search the device provided to Mallory by PRC1, which he had brought to the meeting. At that time, the FBI extracted an image of the device, and returned the device to Mallory. The FBI conducted further technical examination of the imaged copy of the device after the interview.

28. During the May 24, 2017 interview with the FBI, Mallory told the agents that during his most recent trip to the PRC in April 2017, he had been given the device by PRC1 and was trained to use it specifically for private communications with PRC1, an individual he believes works for the PRCIS. Mallory based this assessment on the multiple examples of PRCIS tradecraft and taskings which would be consistent with PRC government officials or intelligence officers (hereinafter "IOs"), and would be inconsistent with the practices of a legitimate commercial company. Mallory told the FBI agents that he was a former U.S. government employee who had training and overseas operational experience, which made it easy for him to spot tradecraft.

29. Mallory told agents that he was encouraged by the PRC IOs to pursue employment with the U.S. Government, which he was already in the process of doing prior to meeting these individuals. When asked where he thought the PRC IOs would like this relationship to go, Mallory told the FBI that he believes they would like to see him obtain a position of access in the U.S. Government.

30. Mallory also told the agents that he received taskings from the individuals he believed were PRC IOs to write papers about U.S. policy matters, and that he responded by writing and delivering two short, unclassified white papers, using information in his head as well as open source information. He stated that he did not retain copies of those documents. Mallory told agents

multiple times that he did not provide the PRC IOs with any other documents in any format, whether in paper or electronic form, beyond these two white papers.

31. Mallory told the FBI agents that he had received cash payments of \$10,000USD in March 2017 and \$15,000USD in April 2017 from the individuals he believed to be PRC IOs. These payments were based on his daily billable rate plus some expenses, and no other payments were due or expected to be paid prior to his anticipated travel in June 2017. In an upcoming trip to the PRC in June, Mallory said that he expected to receive his daily billable rate again. According to Mallory, no payments were due to him from the PRC IOs for work done while Mallory was in the United States.

32. While demonstrating the capabilities of the device at the meeting on May 24, 2017, Mallory voluntarily showed agents how to move from normal message mode to secure message mode. When doing this, Mallory expressed surprise at seeing some secure message history. Prior to the demonstration, he had told the agents that he believed the communication system was designed to delete all previous history. When questioned on the secure messages which were visible on the device, Mallory pointed out to the agents which messages he had sent and which messages PRC1 had sent. One message he had sent stated, "I can also come In the middle of June I can bring the remainder of the documents I have at that time."

33. Upon questioning, Mallory said that comment was a reference to the two white papers he had already told agents about regarding open source U.S. policy information. Mallory stated that the reference to the "remainder of the documents" was just stringing PRC1 along, and that he did not actually have anything to give PRC1.

Passage of Classified Documents Via Device

34. In or around June 2, 2017, upon subsequent technical review of the device that Mallory voluntarily allowed the FBI to search, additional secure message history was recovered. The message history was part of the same string of messages Mallory had shown the FBI agents on May 24, 2017, between himself and PRC1.

35. In a recovered secure message sent from the device on or about May 1, 2017, Mallory wrote, "Also, we may need to go again step by step in my getting the document to become part of the image. Then sending it to you."

36. In messages sent on or about May 3, 2017, PRC1 and Mallory discussed two documents, "no1 and no2," which Mallory had provided to PRC1.

37. During the May 3, 2017 communication, PRC1 wrote, "I suggest you send all and retype the handwriting. And NO1 is obvious the first page of a complete article, where the else is and why it is black on top and bottom....We will try our best to apply for another sum of amount, as you required. However, I'm not sure it will be the same amount for now and I will try, and for safety, we cannot send u in one time or in a short period altogether, need to figure out a better way."

38. In messages sent on or about May 3, 2017, Mallory responded, "The black was to cross out the security classification (TOP SECRET//ORCON//...I had to get it out without the chance of discovery. Unless read in detail, it appeared like a simple note...I have arranged for a USD account in another name. You can send the funds broken into 4 equal payments over 4 consecutive days...When you agree I will send you the bank E.g. instructions."

39. Later in this same conversation, Mallory stated, "It was dicey (look it up) when they asked for me by name. If they we looking for me in terms of State Secrets, and found the SD

card..., we would not be talking today. I am taking the real risk as you, [PRC3], and higher up bosses know... "When you get the OK to replace the prior payment, then I will send more docs. I will also type my notes. NOTE: In the future, I will destroy all electronic records after you confirm receipt...I already destroyed the paper records. I cannot keep these around, too dangerous."

40. In messages sent on or about May 5, 2017, Mallory wrote, "your object is to gain information, and my object is to be paid for." PRC1 responded, "My current object is to make sure your security and try to reimburse you."

41. In messages sent on or about May 5, 2017, Mallory wrote, "I can also come In the middle of June. I can bring the remainder of the documents I have at that time."

42. Analysis of the device revealed a handwritten index describing eight different documents. Four of the eight documents on this list were found stored on the device.

43. USGA1 analyzed the four documents found on the device and confirmed that three of the documents are USGA1 documents, containing classified information. USGA1 further confirmed that one of the three documents was classified at the TOP SECRET level at the time it was transmitted to PRC1 in early May 2017 and continues to be classified at that level. USGA1 further confirmed that the remaining two documents were classified at the SECRET level at the time they were transmitted to PRC1 in early May 2017 and continue to be classified at that level.

CHARGES

False Statements – 18 U.S.C. § 1001

44. Mallory made materially false statements during the FBI interview on May 24, 2017 in Ashburn, Virginia. After being informed of the identities of federal agents, Mallory knowingly and willfully made numerous materially false statements about sending documents to presumed PRC IOs, including by:

- Claiming to FBI agents that he had not provided additional documents, beyond two unclassified white papers, to individuals he identified as PRC IOs.
- Claiming to FBI agents that he had never transmitted documents, other than a test message, using the device.

Delivering Defense Information To Aid Foreign Government – 18 U.S.C. § 794

45. With reason to believe it would be used to the injury of the United States or to the advantage of the PRC, Mallory transmitted national defense information in the form of documents classified at the SECRET and TOP SECRET level to an agent of the PRC.


CONCLUSION AND SEALING REQUEST

46. For all the reasons stated above, there is probable cause to believe that from in or about April 2017 through in or about May 2017, Mallory made materially false statements to federal law enforcement officers, in violation of 18 U.S.C. § 1001, and transmitted national defense information to an agent of the PRC in violation of 18 U.S.C. § 794. These criminal violations were either begun or committed in the Eastern District of Virginia, or were begun or committed overseas, out of the jurisdiction of any particular state or district, and your affiant expects that Mallory will be arrested in the Eastern District of Virginia.

47. I ask that this affidavit be sealed, until further order of the court, to protect this investigation. I am aware from my training and experience that evidence is destroyed, individuals flee, and witnesses may be tampered with or become uncooperative when the details known to law enforcement become prematurely available to the targets of a criminal investigation.


48. I declare under the penalty of perjury that the information provided above is true and correct.

Respectfully submitted,



Stephen Green
Special Agent
Federal Bureau of Investigation
Washington, D.C.

Subscribed and sworn to before me
on June 24, 2017.



Theresa Carroli Buchanan
United States Magistrate Judge

THE HONORABLE THERESA C. BUCHANAN
UNITED STATES MAGISTRATE JUDGE